

Contro i “tre mali” la Sco si fa cyber

L'antiterrorismo guidato dalla Cina in Asia centrale si rafforza aprendo un fronte virtuale

Stefano Sartorio



Il concetto dei “tre mali” o delle “tre forze malvagie” (*sangu shili*) viene utilizzato spesso dalla retorica del Partito comunista cinese (Pcc) in tema di lotta al terrorismo. Esso identifica le tre minacce che la leadership cinese vorrebbe eliminare: il terrorismo, il separatismo e l'estremismo. In particolare, si può riscontrare come in realtà queste vengano percepite all'interno di un unico ombrello che racchiude le più grandi preoccupazioni dello Stato, che minacciano il governo del partito unico e la stessa unità territoriale del Paese. Con l'istituzione, nel 2001, della Shanghai Cooperation Organization (Sco) si delinea l'inizio di una strategia di cooperazione regionale (comprendente oggi il sub continente Indiano, l'Asia Centrale, la Cina e la Russia) allo scopo di arginare i succitati pericoli attraverso una chiave di lettura comune. All'interno di questo organismo negli ultimi cinque anni si è dunque sviluppata una nuova strategia di interdizione nei confronti dei gruppi inseriti all'interno delle tre categorie. Lo spazio dei “tre mali” travalica i confini del “reale” per fluire in quello del “virtuale”.

«La rete va governata come gli stati»

La cyberizzazione della Sco risale all'accordo del 16 giugno 2009 sulla cooperazione per garantire la sicurezza informatica tra gli Stati membri dell'Organizzazione. All'interno del testo vengono infatti enucleate le minacce nel settore della “sicurezza informatica” (degli individui, della società e dello Stato nello spazio informatico) tra le quali rientrano fattispecie di natura molto varia: dalla manipolazione delle informazioni alla criminalità informatica.

Questo approccio è testimone dell'influenza cinese sull'Organizzazione e sull'accento posto da Pechino sulla necessità di garantire a livello regionale un controllo informatico complessivo e ferreo. Si parla così di “sovranità di internet” (*wangluo zhuquan*): in sostanza la concezione secondo la quale anche la rete dovrebbe essere governata dalle leg-

gi che regolamentano le relazioni tra Stati. Analizzando la National Defense Strategy del 2006 e considerando anche le parole di Xi Jinping durante l'inaugurazione del “Central Internet Security and Informatization leading group” del 28 febbraio del 2014 («Senza sicurezza di internet non esiste alcuna sicurezza nazionale. Senza informatizzazione non esiste modernizzazione») risulta evidente che il controllo e la sicurezza della rete viene collegato direttamente al mantenimento della sicurezza nazionale.

All'interno della strategia cinese per il cyberspazio si interpone come obiettivo fondamentale la “supremazia informativa” (*zhi xinxi quan*) e la conseguente “sicurezza dell'informazione” (*xinxi anquan*), principio che identifica il dominio su tutte le fonti di informazione, compresi i social media, dove la propaganda politica e il desiderio da parte della società civile di ottenere informazioni entrano spesso in conflitto. La capacità di produrre, diffondere e controllare le informazioni, anche oltre i confini nazionali, è un interesse fondamentale per la Cina. In questa intersezione tra sicurezza interna e vulnerabilità virtuale si colloca la volontà del Paese di costruire una formula per identificare le “minacce” alla propria stabilità.

Questo approccio ha avuto applicazione all'interno delle attività della SCO. Nel 2015, 2017 e 2019 si sono tenute a Xiamen (nella provincia del Fujian) tre esercitazioni congiunte nel cyberspazio (*wangluo yanxi*) tra i membri dell'organizzazione. Esse hanno avuto lo scopo di migliorare le capacità investigative e di prevenzione nell'uso di Internet per contrastare la propaganda e l'influenza dei

La Shanghai Cooperation Organization (Sco) fu fondata il 15 giugno 2001 a Shanghai. I suoi obiettivi principali sono: mantenere e assicurare la pace, la sicurezza e la stabilità della Regione; promuovere la cooperazione politica e commerciale; rafforzare la fiducia e incoraggiare lo sviluppo delle relazioni tra gli stati membri.

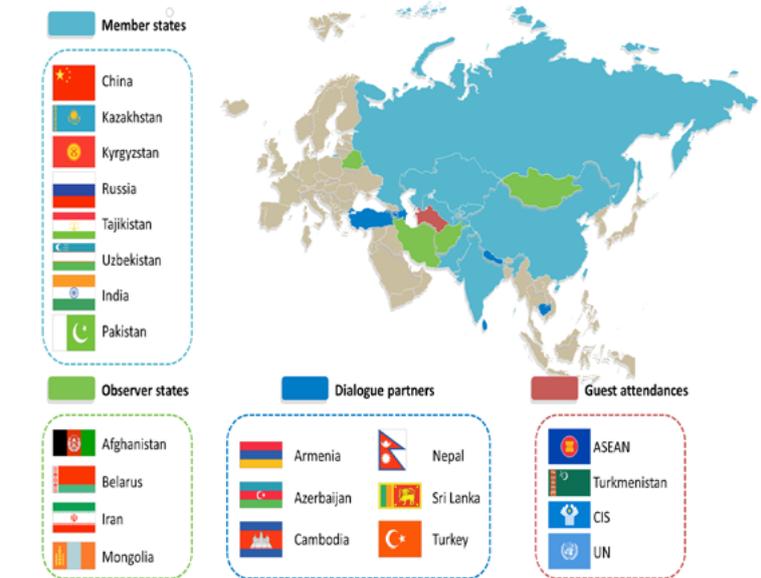
“tre mali”. Le operazioni sono state dirette dalla SCO Regional Anti Terrorist Structure (Rats), con sede in Tashkent (Uzbekistan), apparato dell’Organizzazione con lo scopo di promuovere la cooperazione nel settore. Queste esercitazioni sono consistite nell’intercettare propaganda terroristica o estremista e nel bloccarne la diffusione. All’interno dell’ultima esercitazione del 2019, le forze armate congiunte hanno anche sviluppato metodi in cooperazione per la ricerca e la cattura degli individui responsabili delle stesse.

Il separatismo si combatte online

Il Cyber-terrorismo, il cyber-estremismo e il cyber-separatismo sono dunque i tre nuovi nemici da contrastare per la Sco e per la Cina stessa, che come abbiamo visto in tema di cyber sicurezza ha avuto una forte influenza sia nella definizione dei termini utilizzati che nella filosofia normativa. Il cyber-separatismo concettualmente nasce da una definizione di Dru C. Gladney ripresa all’interno del suo libro *Dislocating China, Muslims, Minorities and other subaltern subjects* nel quale cui descrive il processo tramite il quale, all’interno della comunità uigura cinese, nella rete hanno preso corpo voci di dissenso e fermenti autonomisti.

Lo spostamento progressivo della protesta di piazza verso la sfera virtuale alla fine degli anni Novanta avrebbe creato un ulteriore problema al Pcc, poiché in questo modo i vari movimenti separatisti hanno aumentato la loro capacità di proselitismo, raggiungendo centinaia di migliaia di soggetti, potendo così riunire la maggior parte delle comunità uigure del mondo. Molte organizzazioni che sostengono l’indipendenza della regione del Turkestan orientale poi hanno sede all’estero, ad esempio a Monaco di Baviera, Istanbul e negli Stati Uniti. Il gruppo Etim (East Turkestan Islamic Movement) - sulla struttura, organizzazione e rilevanza del quale gli esperti di terrorismo sono divisi - su pressioni di Pechino è stato riconosciuto come “organizzazione terroristica” dalle Nazioni unite.

Il cyber-terrorismo ed il cyber-estremismo sono invece fenomeni più comprensibili sviluppatasi negli ultimi anni e possono essere considerati uno come conseguenza dell’altro. Mentre il primo, generalmente, prevede azioni reali di manipolazione delle reti informatiche per creare danni tangibili ad infrastrutture, persone o reti allo scopo di generare terrore, il secondo ha un connotato differente. Secondo quanto riportato da una ricerca condotta da Imran Awan, *Cyber-Extremism: Isis and the Power of Social Media*, infatti, i siti Internet e i social media agiscono come echo chamber ideali alla promozione della violenza come strategia (di dissenso). Gli individui apprendono così comportamenti devianti da gruppi o persone, con-



vogliando un estremismo categorizzato da associazioni, definizioni, rinforzi differenziali e imitazioni. Gli individui cosiddetti recruiter utilizzerebbero quindi la rete per radicalizzare soggetti vulnerabili per l’esecuzione e il sostenimento di comportamenti criminali per lo Stato (i.e. Al Hayat Media Centre, direttamente collegato a Isis).

Conclusioni

Le minacce percepite all’unità del Paese motivano l’azione del governo e conseguentemente le sue azioni all’interno della Sco, organizzazione che sembra evolversi intorno ai concetti e alle sfide chiave della Cina. Insieme ai membri dell’Organizzazione, il paese sta quindi sviluppando un framework normativo ed interpretativo che possa guidare le proprie azioni nell’ambito cibernetico, strutturando un processo di contrasto nei confronti di individui e gruppi in grado di minacciare le sue strategie nazionali nel teatro virtuale. Oltretutto, date le definizioni non condivise a livello internazionale e a volte generali in merito ai “tre mali”, il paese potrebbe così contribuire ad allargare le maglie terminologiche per evidenziare circostanze di illiceità più favorevoli alle esigenze di sicurezza nazionale all’interno di un settore ancora indefinito come quello virtuale.

Stefano Sartorio è laureato in Relazioni Internazionali all’Università degli studi di Milano.